\Orchestrating a brighter world NEC

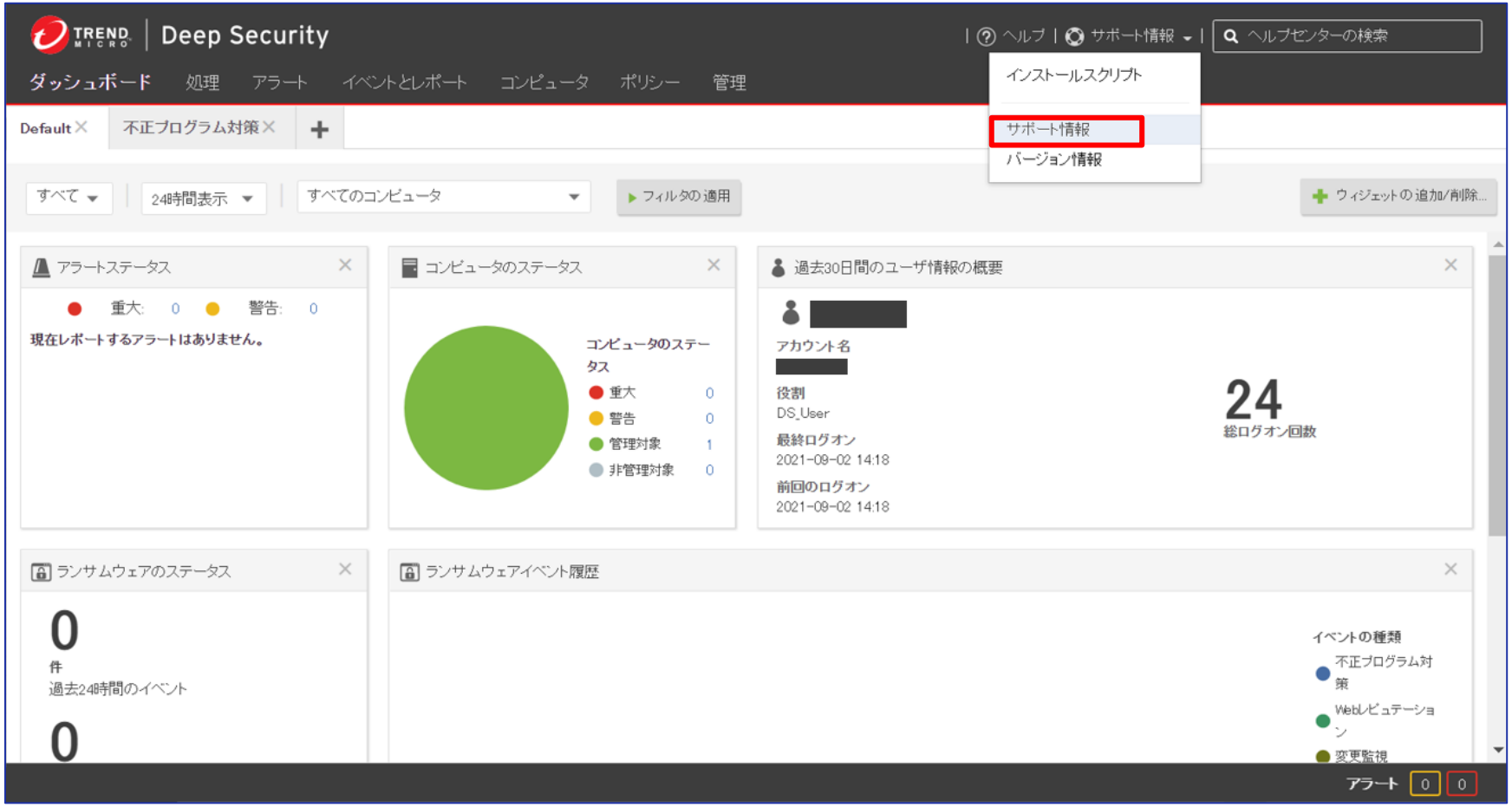
Deep Security Agent ユーザーズガイド 第7版

2024年 8月 日本電気株式会社

目次

概要

- 本資料はサーバセキュリティサービス利用者向けガイドになります。
- 詳細につきましては、サポート情報にてご確認お願いします。



1.ログイン

◆ ログイン手順

- サーバセキュリティサービスのDeep Securityは、
  Webブラウザで管理コンソールにアクセスして管理します。

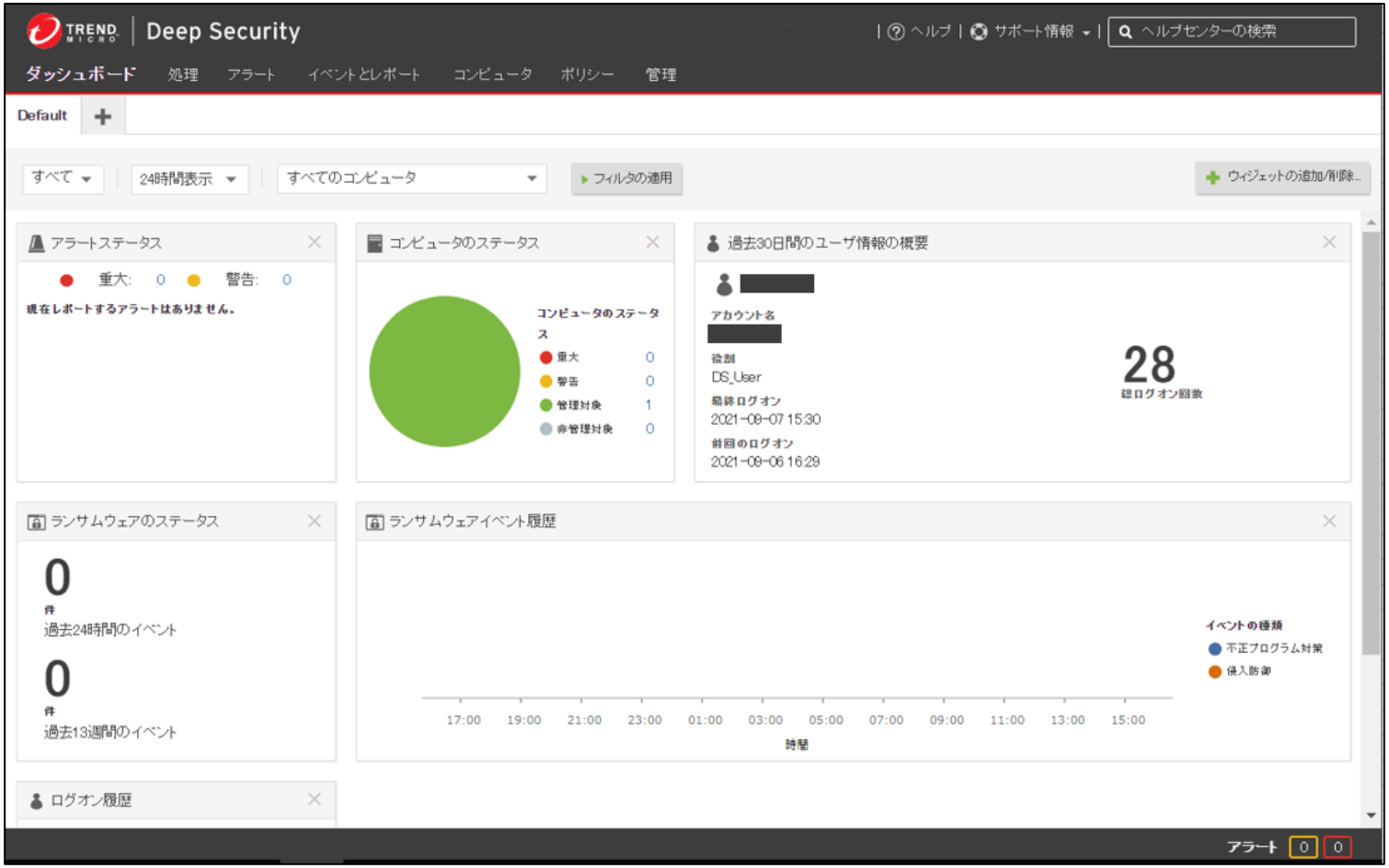
■ ログイン手順は以下となります。

[1] https://serversecurity-nec.jp/SignIn.screenにアクセスして下さい。
[2]「アカウント名」「ユーザ名」「パスワード」を入力してログイン。
※初期設定はライセンス証書に記載されています。

2.ダッシュボード

◆ 概要

- [ダッシュボード]には、システムの状態を一目で理解できるビューがあります。これらの表示項目などは、自由に変更できます。

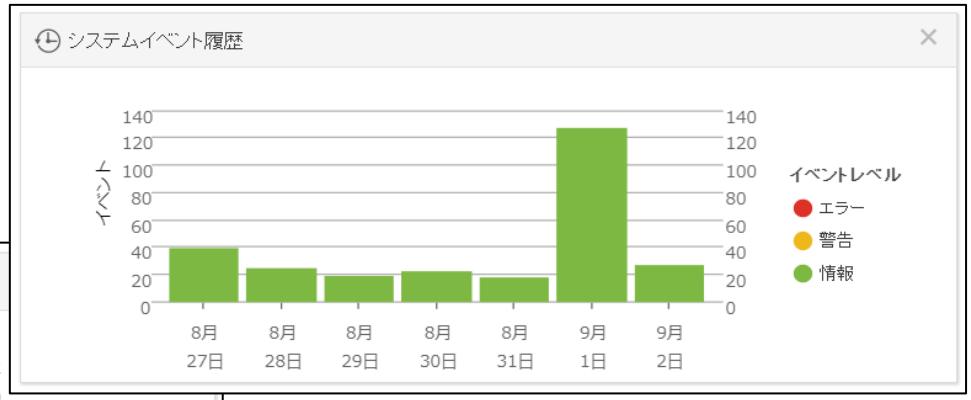


2.ダッシュボード

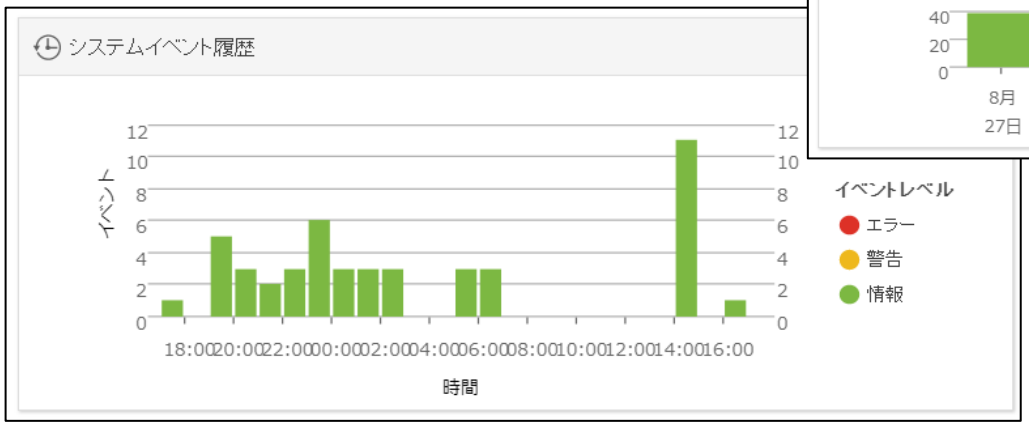
◆ 表示期間の変更

ウィジェットの日時表示範囲を24時間表示 or 7日間表示に切り替えることができます。

7日間表示

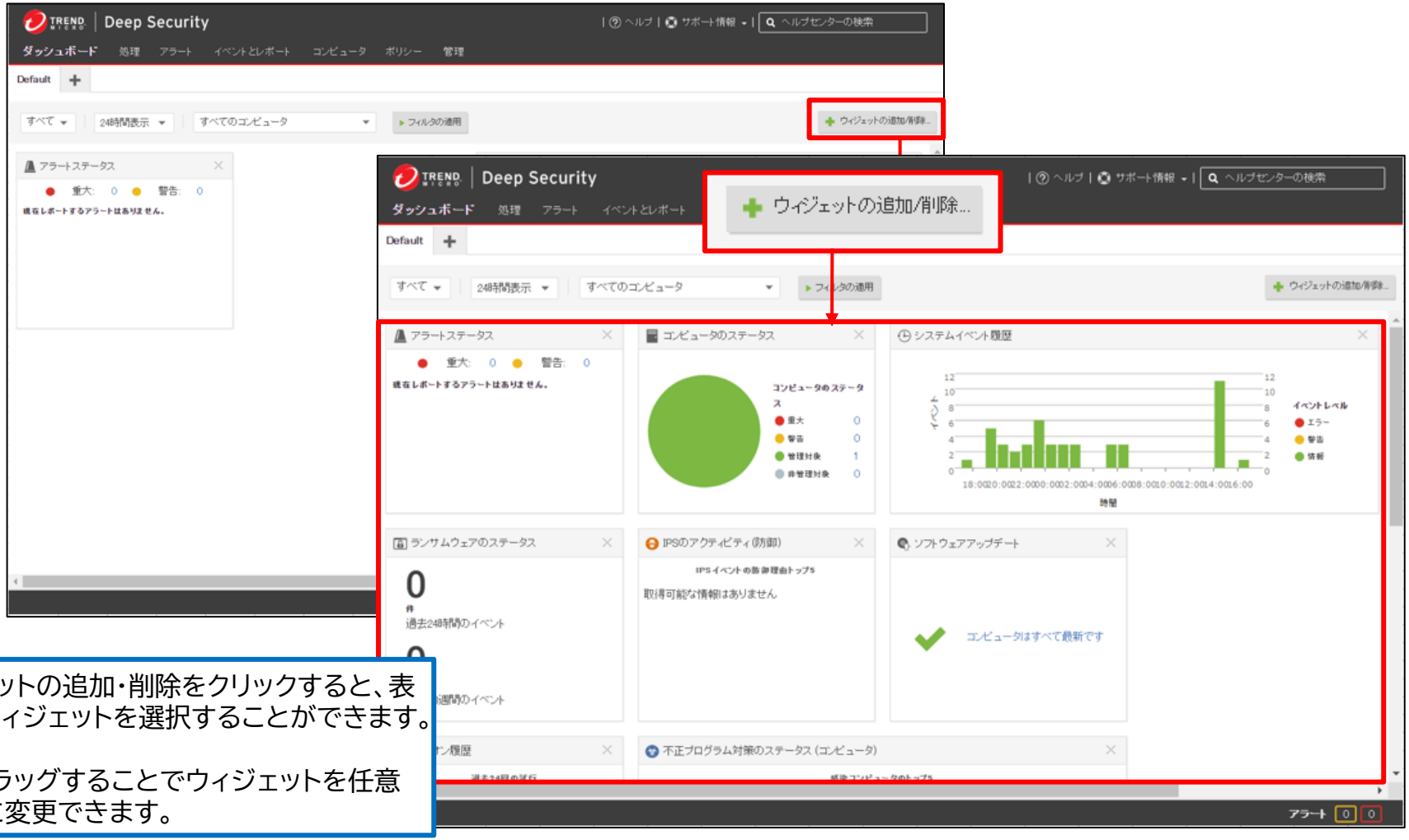


24時間表示



2.ダッシュボード

- ウィジェット(表示項目)の追加・削除



ウィジェットの追加・削除をクリックすると、表示するウィジェットを選択することができます。

また、ドラッグすることでウィジェットを任意の配置に変更できます。

2.ダッシュボード

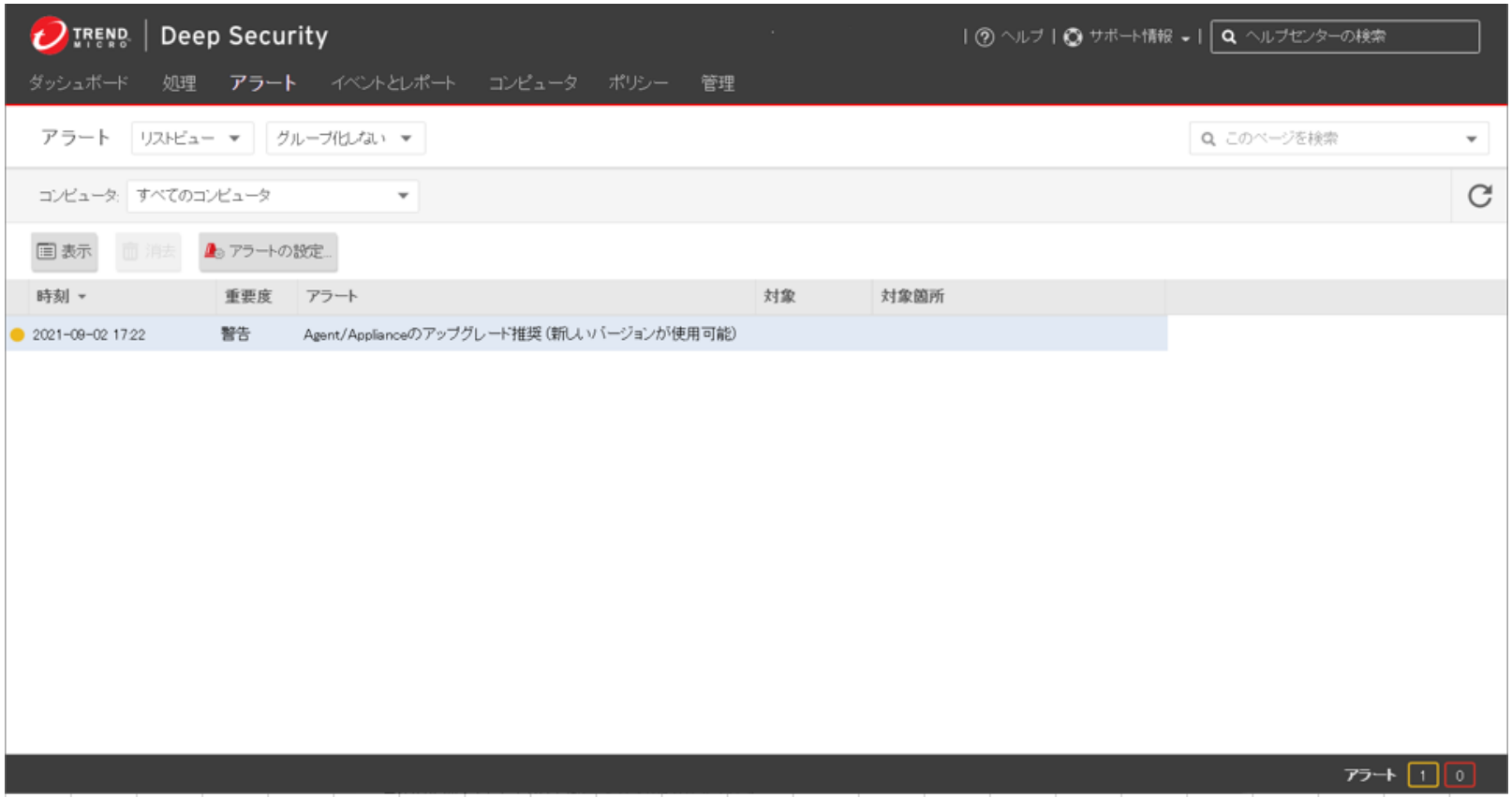
◆ タブの追加

[+]をクリックし、タブを追加する事で、
機能毎に表示項目を分けるなど
カスタマイズ可能です。

3.アラート

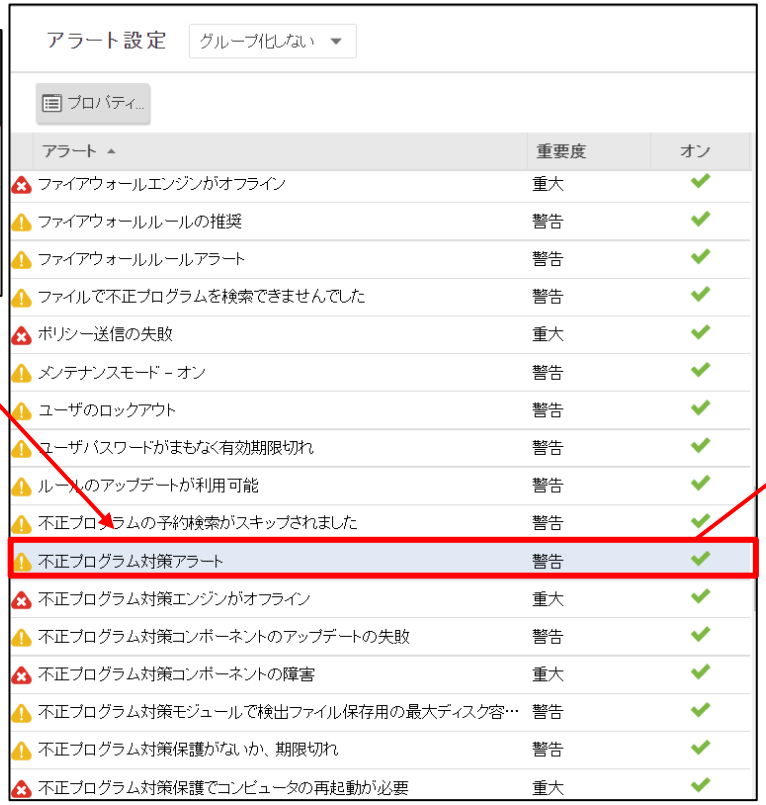
◆ 概要

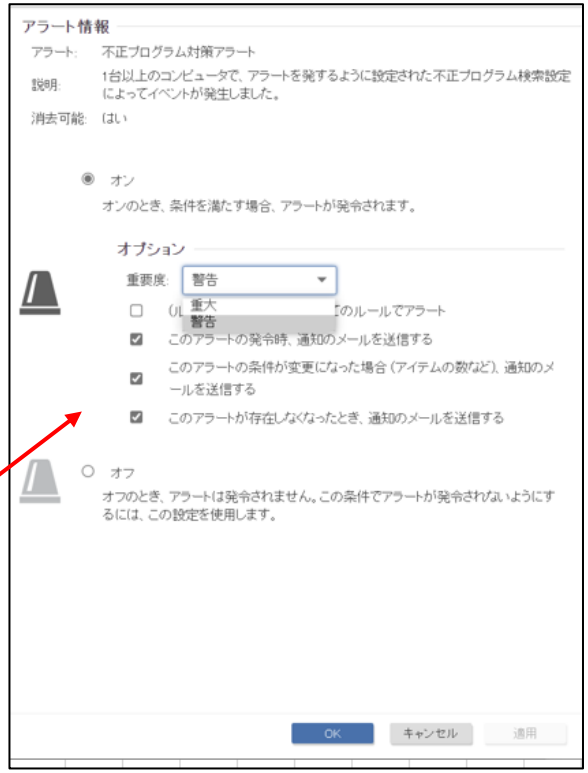
- [アラート]画面には、有効なアラートがすべて表示されます。
  [アラートの設定]を行うことで、表示有無や重要度を任意に変更できます。



3.アラート

◆ アラートの設定

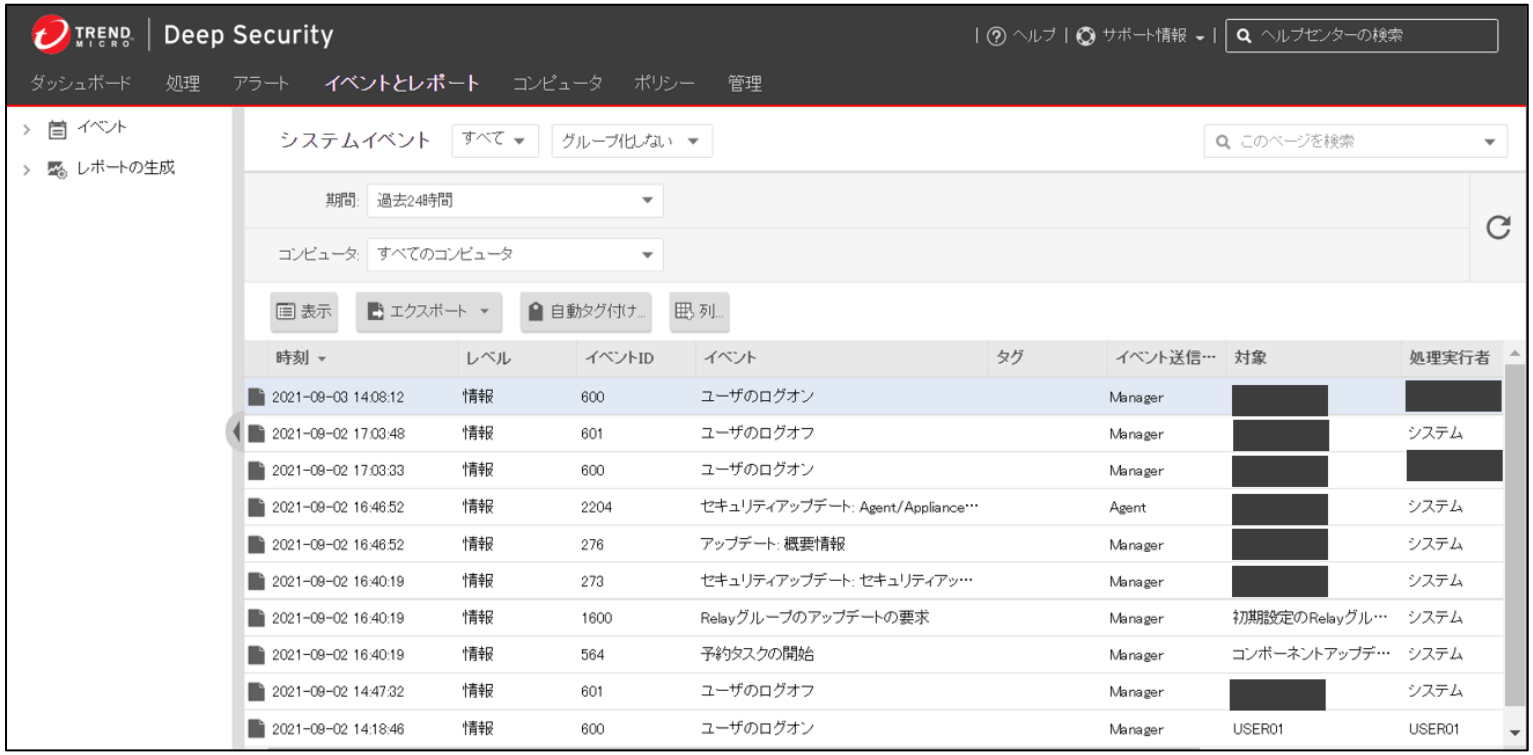




4.イベントとレポート

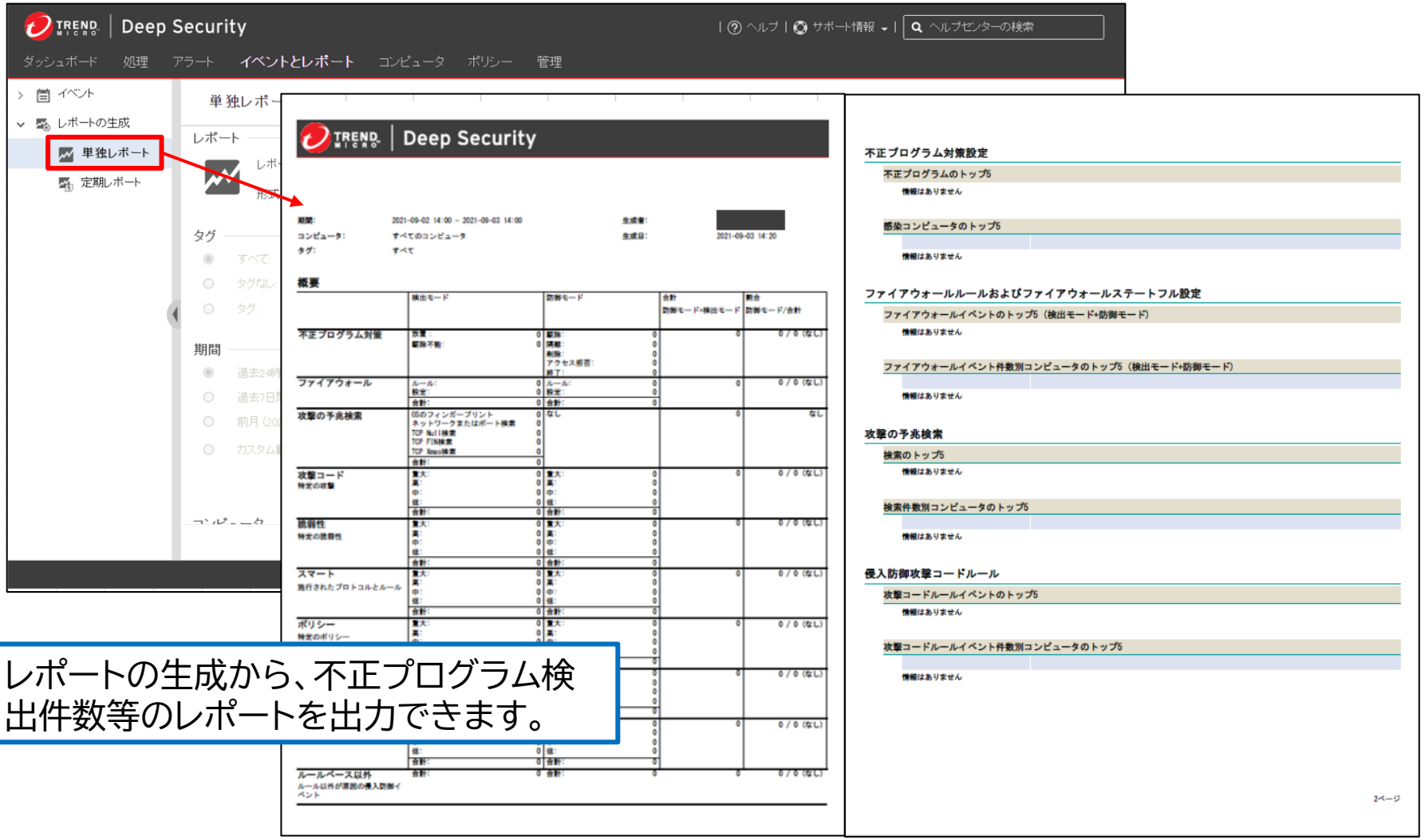
◆ 概要

- [イベントとレポート]では、各種イベントの表示、レポートの作成を行えます。



4.イベントとレポート

◆ レポートの作成



レポートの生成から、不正プログラム検出件数等のレポートを出力できます。

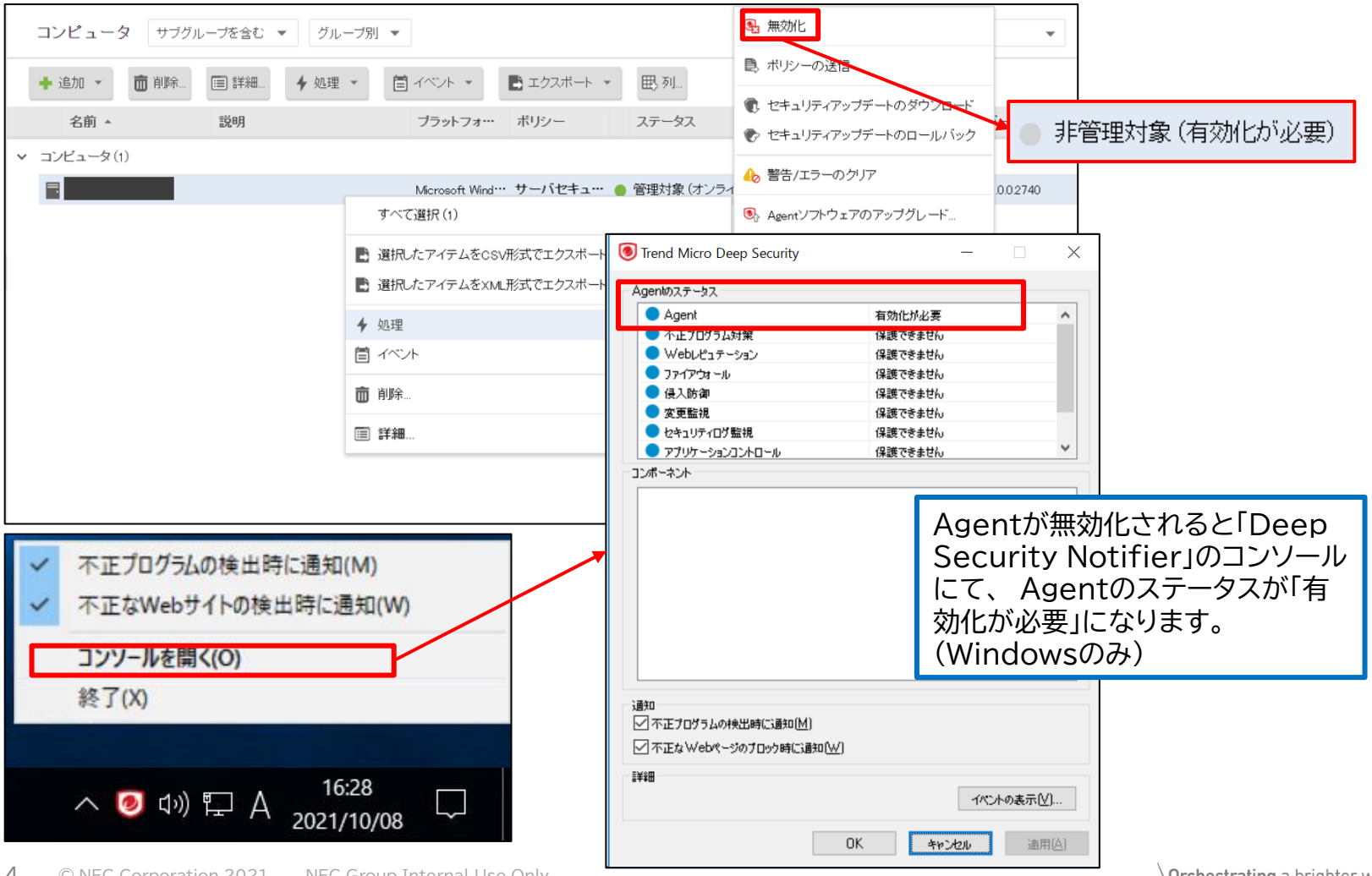
5.コンピュータ

◆ 概要

- [コンピュータ]では、推奨スキャンの実施や表示名変更など各コンピュータの管理を行います。

5.コンピュータ

- Agentの無効化
  - 処理＞無効化より、Agentを無効化できます。



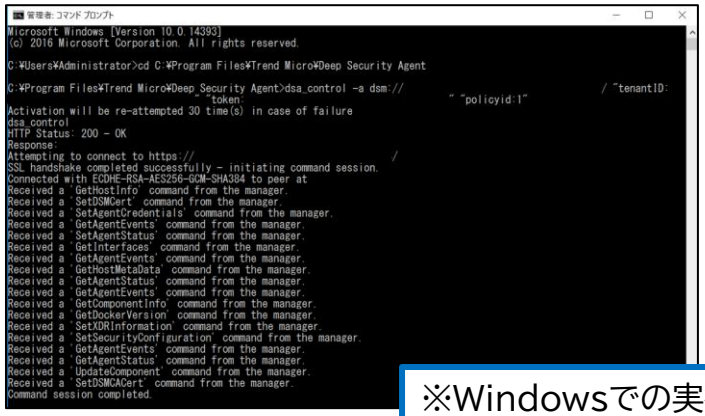
5.コンピュータ

- Agentの有効化
- 無効化したAgentを有効化する場合は、対象のサーバ上で有効化コマンドを実行する必要があります。

[1]有効化コマンドの作成

※手順は導入手順書を確認

[2]有効化するサーバ上で有効化コマンドを実行する。



※Windowsでの実行例

5.コンピュータ

- グループの設定
- 管理コンソール左側のコンピュータを右クリックすることで
  新規にグループを追加できます。
- グループを割り当ては、コンピュータの詳細(対象をダブルクリック)
  より行います。

5.コンピュータ

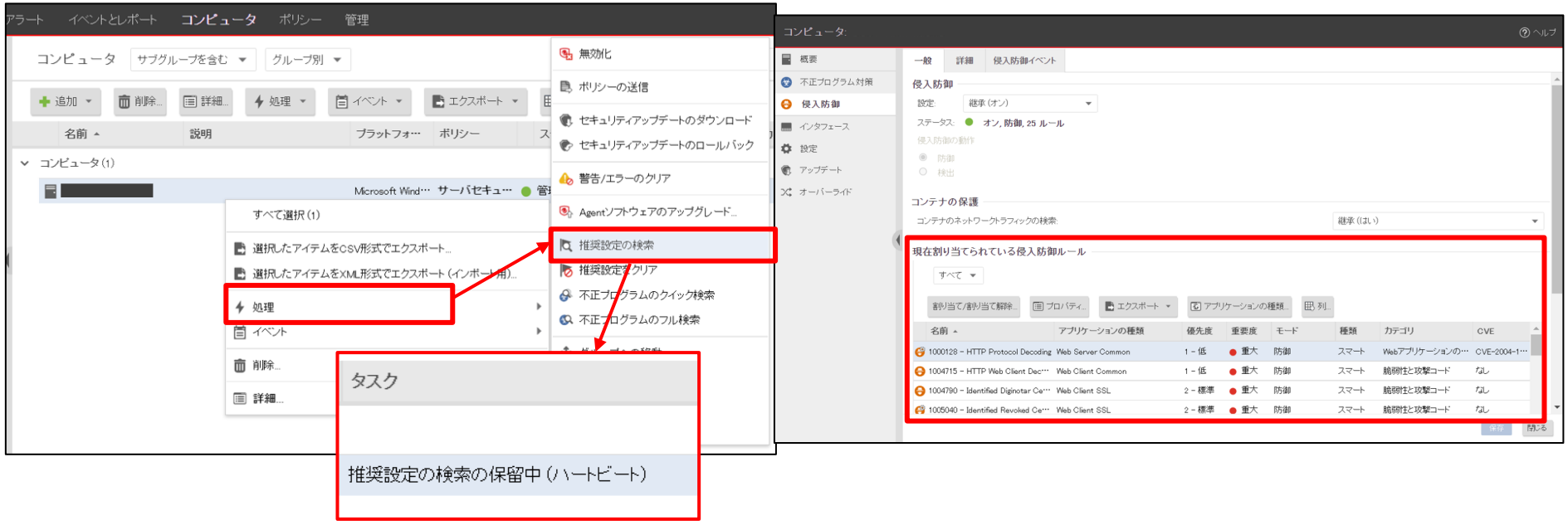
◆ 推奨スキャンの実施

[1]「コンピュータ」タブより、対象サーバを右クリック。

[2]処理＞推奨設定の検索をクリック。

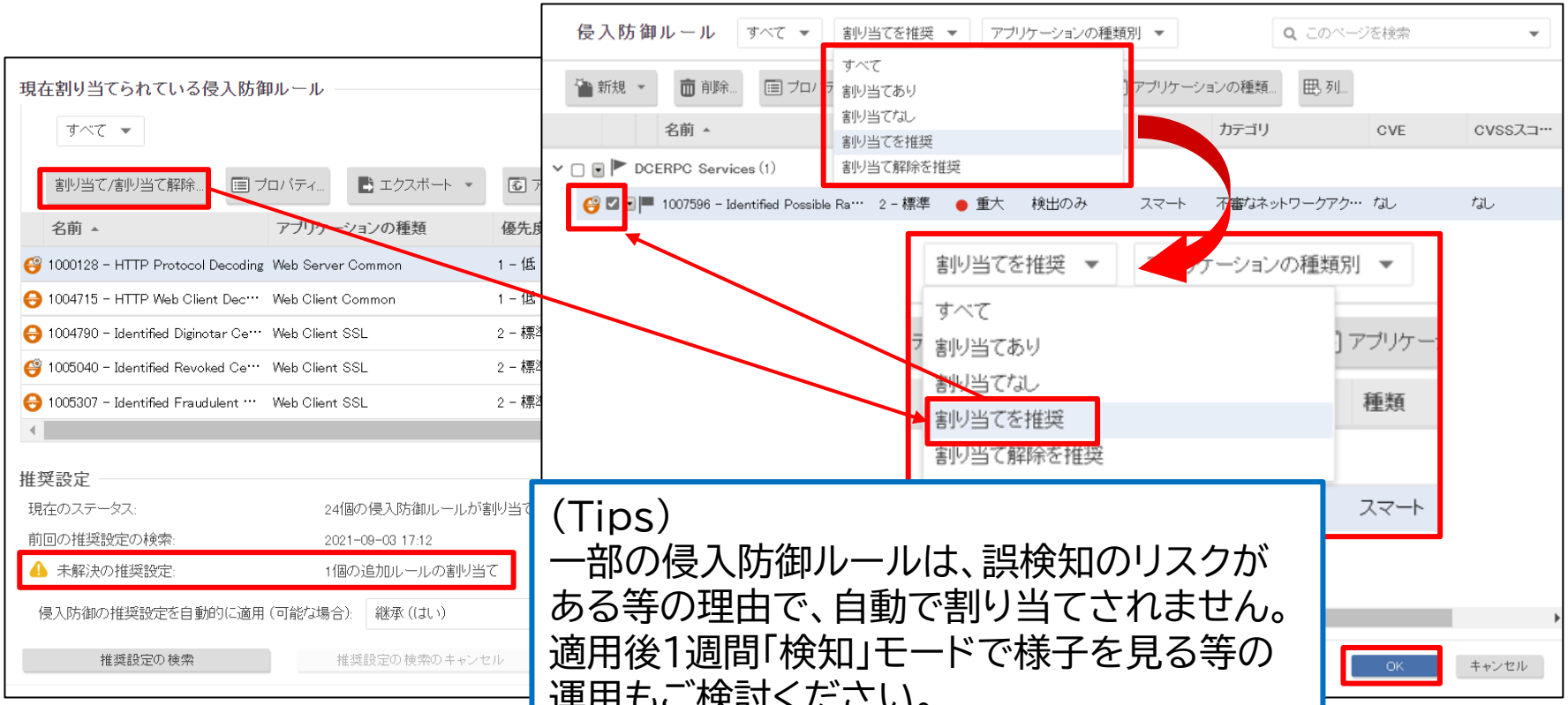
[3]ステータス列に「推奨設定の検索の保留中（ハートビート）」が表示され、
数分後に推奨設定が実行されます。

[4]推奨スキャン実施後、対象コンピュータをダブルクリックし、侵入防御を選択。一般タブにて
割り当てられている侵入防御ルールを確認できます。



5.コンピュータ

- 推奨スキャン完了後、「未解決の推奨設定」がある場合は下記の手順でルールの割当てが可能です。※自動的に適用できないルールがございます。
  [1]「割り当て/割り当て解除...」をクリック。
  [2]侵入防御ルールの中央のボックスから「割り当てを推奨」を選択
  [3]表示されたルールの左側のチェックボックスをチェックして、OKボタンを押す。



（Tips）
一部の侵入防御ルールは、誤検知のリスクがある等の理由で、自動で割り当てされません。
適用後1週間「検知」モードで様子を見る等の運用もご検討ください。

6.ポリシー

- 概要
- ポリシーの確認・編集や、侵入防御ルールの確認等を行えます。

6.ポリシー

- ポリシーの継承
- 親ポリシーを元に作成された子ポリシーは、設定変更しない場合、ポリシー設定画面にて「(継承)」と表記されます

6.ポリシー

◆ 侵入防御ルール手動適用の注意点

■推奨設定の検索使用時に任意のルールを手動で割り当てする場合

推奨設定の検索にて、[侵入防御の推奨設定を自動的に適用（可能な場合）:]を「はい」に設定している場合、コンピュータの詳細画面から、コンピュータレベルで手動適用した侵入防御ルールが、自動的に割り当て解除される場合があります。

推奨設定の検索使用時に任意のルールを手動で割り当てする場合は、
ポリシーの設定画面から、ポリシーレベルで任意のルールを割り当ててください。

参考情報
https://success.trendmicro.com/ja-jp/solution/ka-0001819

6.ポリシー

[侵入防御の推奨設定を自動的に適用（可能な場合）:]の設定は、
「ポリシー」または「コンピュータ」の詳細ページで確認できます。
・「ポリシー」→対象のポリシーをダブルクリックして詳細画面を表示。
・「コンピュータ」→対象のコンピュータをダブルクリックして詳細画面を表示。
→左ペインの「侵入防御」を選択し、「一般」タブを参照する。（共通）

6.ポリシー

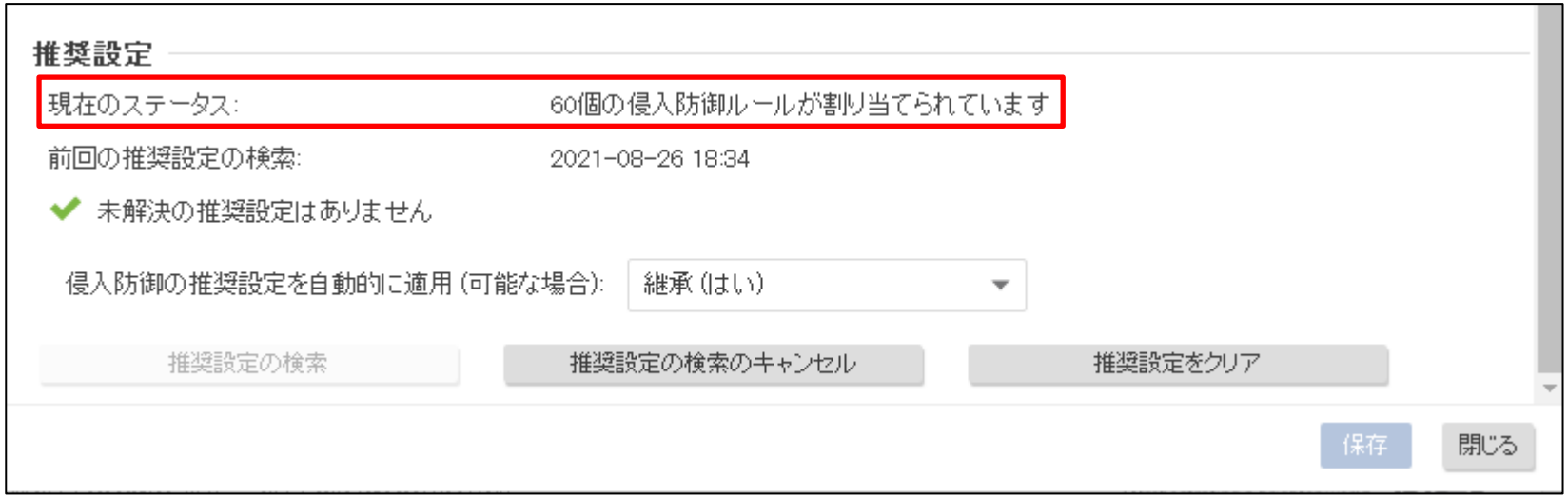
◆ 侵入防御ルールを手動適用する手順

1. 現在割り当てられているルールの確認

侵入防御ルールを手動適用した後、割り当てられていることを確認するために、以下の手順で対象のコンピュータの詳細画面を開き、現在割り当てられている侵入防御ルールの数と、割り当てるルールの適用状況、設定状況が分かるように、メモまたは画面キャプチャの取得をしてください。

- 現在割り当てられている侵入防御ルールの数の確認

[コンピュータ] → 対象のコンピュータの[詳細]→ [侵入防御] → [一般]タブを参照



6.ポリシー

- 割り当てるルールの適用状況の確認

対象のコンピュータの[詳細]から、以下の手順でルールの適用状況を確認。

6.ポリシー

- 割り当てるルールの設定状況の確認

ルールの設定を変更される場合は、対象のルールの[プロパティ]を開き、現在の設定状況がわかるように、メモまたは画面キャプチャを取得してください。

6.ポリシー

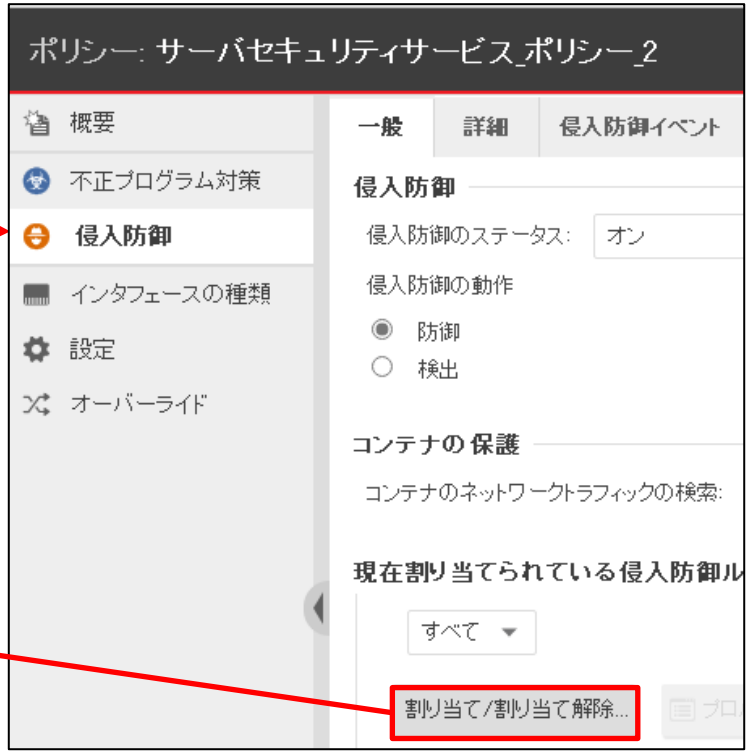
2. [サーバセキュリティーサービス_ポリシー]を複製

[ポリシー]タブ→[ポリシー]

6.ポリシー

3. 複製したポリシーに侵入防御ルールを割り当てる

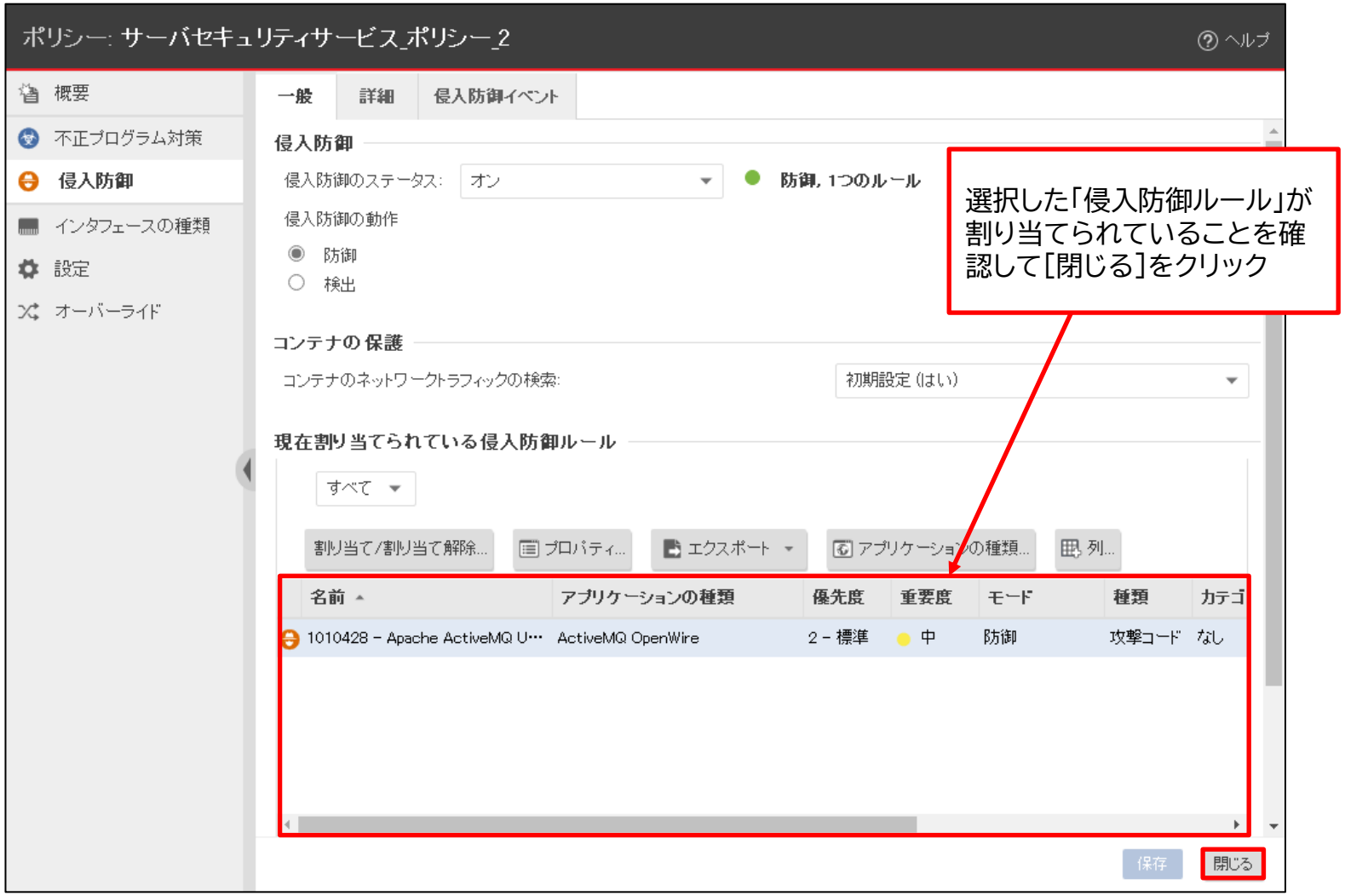
作成したポリシーを右クリックし、詳細をクリック



割り当てたい侵入防御ルールにチェックを入れて[OK]をクリック

[侵入防御]の一般タブにある[割り当て/割り当て解除]をクリック

6.ポリシー

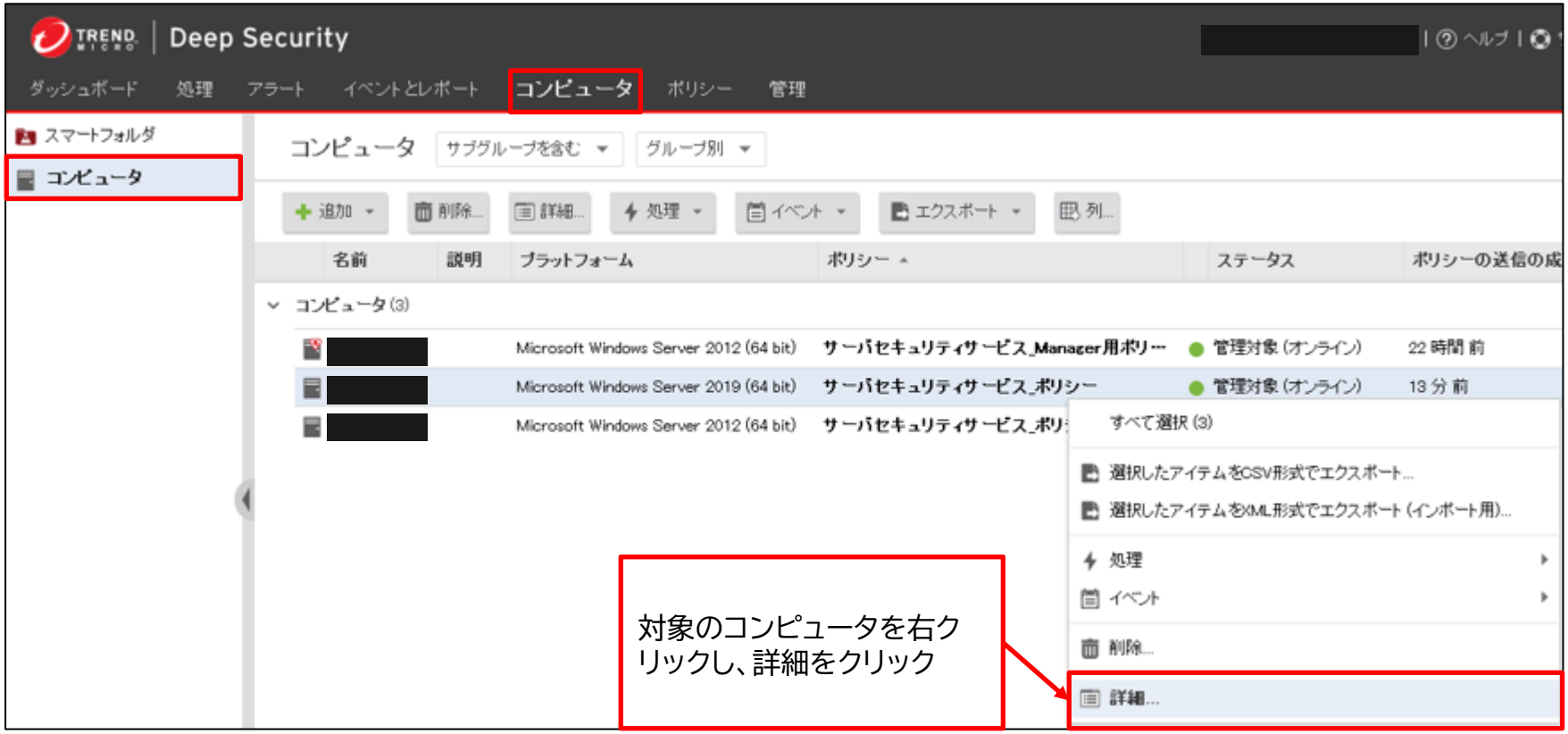


6.ポリシー

4. 複製したポリシーを対象のコンピュータに適用する

コンピュータにポリシーを適用した段階で、ポリシーに割り当てたルールがDSAに反映されます

- 対象コンピュータの詳細を表示します。



6.ポリシー

- [概要] → [一般] タブの [ポリシー:] のプルダウンから作成したポリシーを選択して保存することで、DSA へ自動でポリシーが配信され、ポリシー適用後に割り当てたルールが DSA へ反映されます。

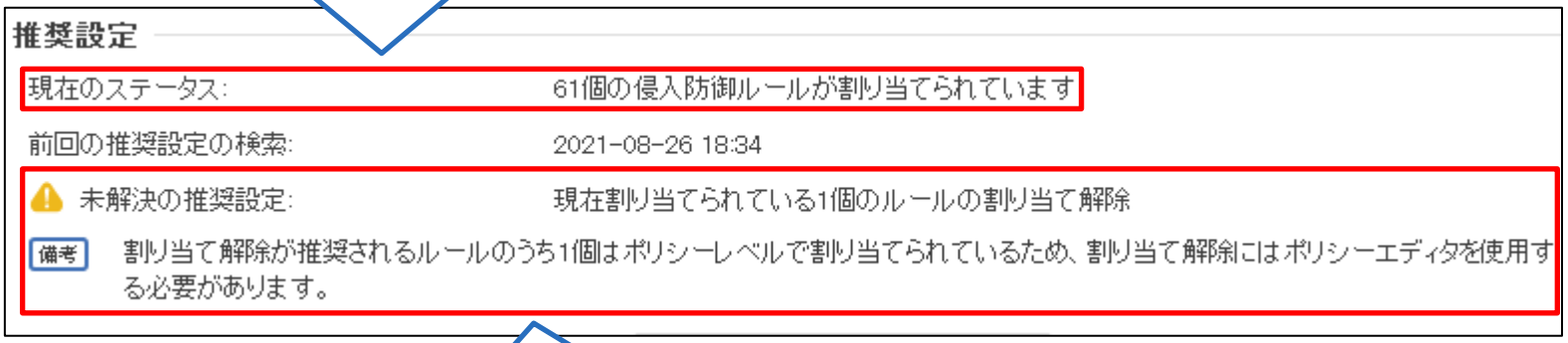
6.ポリシー

5. ポリシーで割り当てたルールが適用されていることを確認

- 現在割り当てられている侵入防御ルールの数の確認

対象のコンピュータの[詳細] → [侵入防御] → [一般] → [推奨設定]を確認

[現在のステータス:]が、手順1で取得した画面キャプチャまたはメモと比較し、手順3で割り当てたルールの数だけ増えていることを確認



推奨設定の検索によって解除されているルールを適用すると、[未解決の推奨設定:]が表示されます。

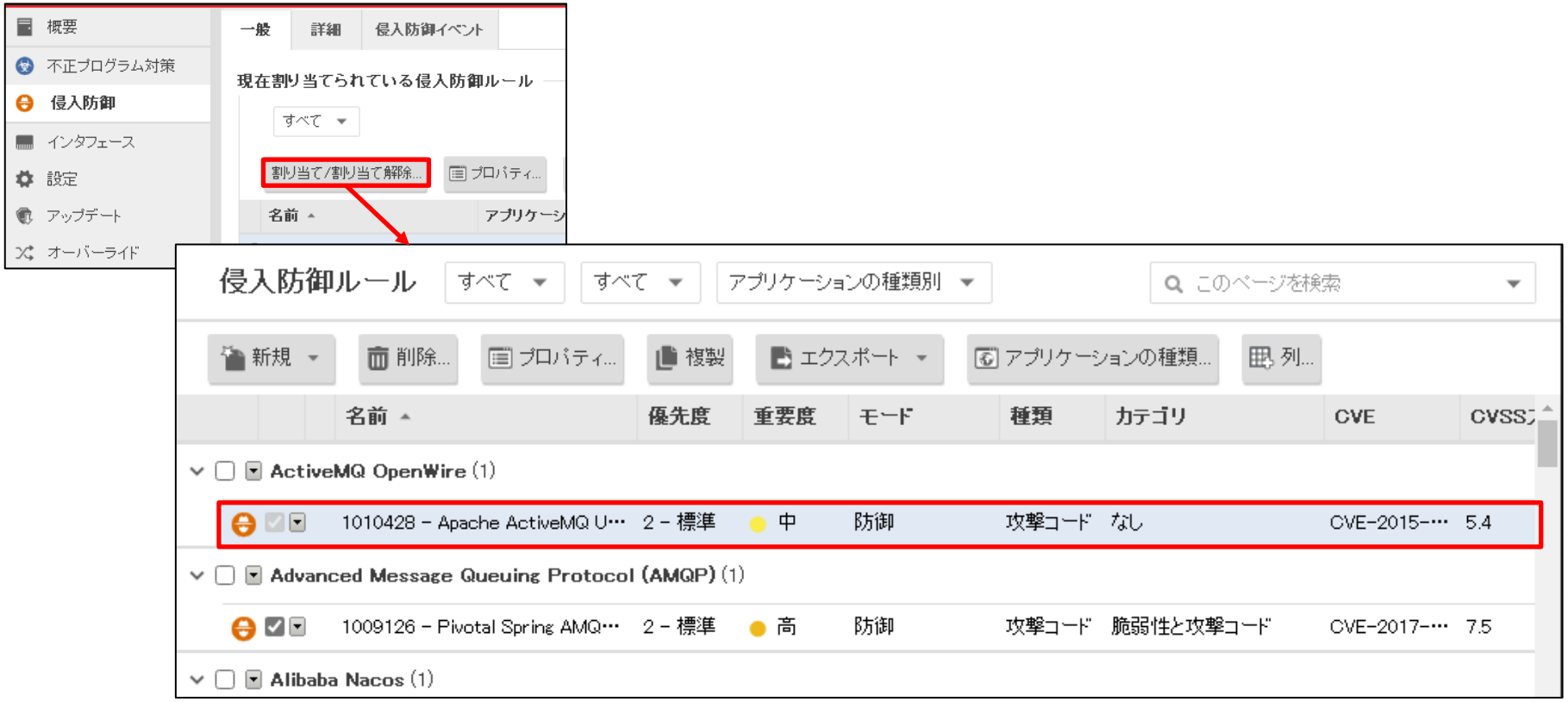
[備考]には、手順3でポリシーに割り当てたルールの数が表示されます。

6.ポリシー

- 割り当てたルールの適用状況の確認

[割り当て/割り当て解除]をクリックし、手順1で取得した画面キャプチャまたはメモと比較して意図したルールにチェックが入っていることを確認。

ポリシーによって割り当てられたルールのチェックボックスはグレーアウトされ、コンピュータからは解除できないようになっています。



6.ポリシー

- 割り当てたルールの設定状況の確認

ルールの設定を変更された場合は、対象のルールをダブルクリックしてプロパティを開き、変更した設定項目を確認し、手順1で取得した画面キャプチャまたはメモと比較して意図した設定になっていることを確認。

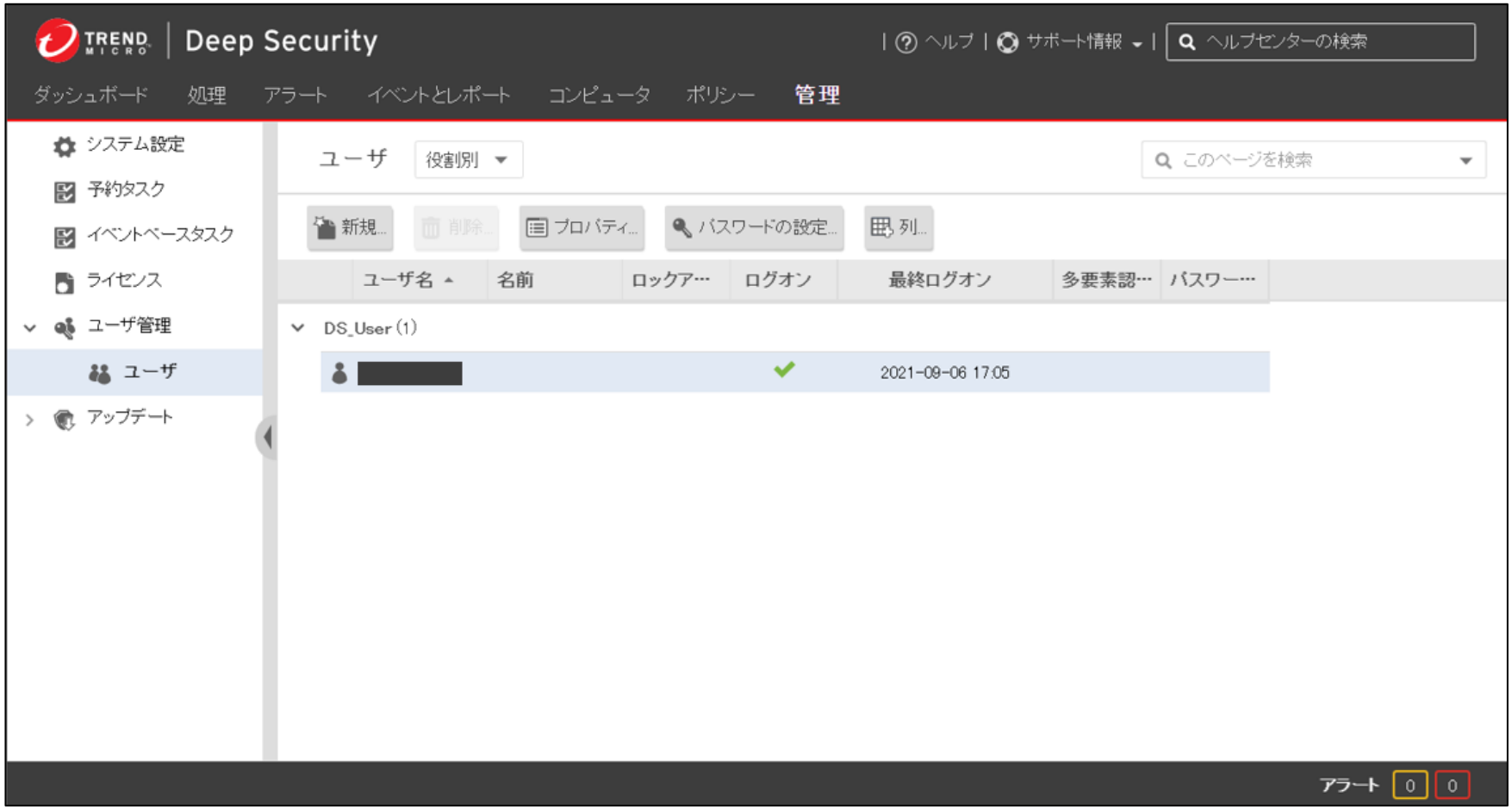
7.管理

◆ 概要

- [管理]では、ライセンスの確認やログインユーザの管理、
  ソフトウェアのアップデートを行えます。

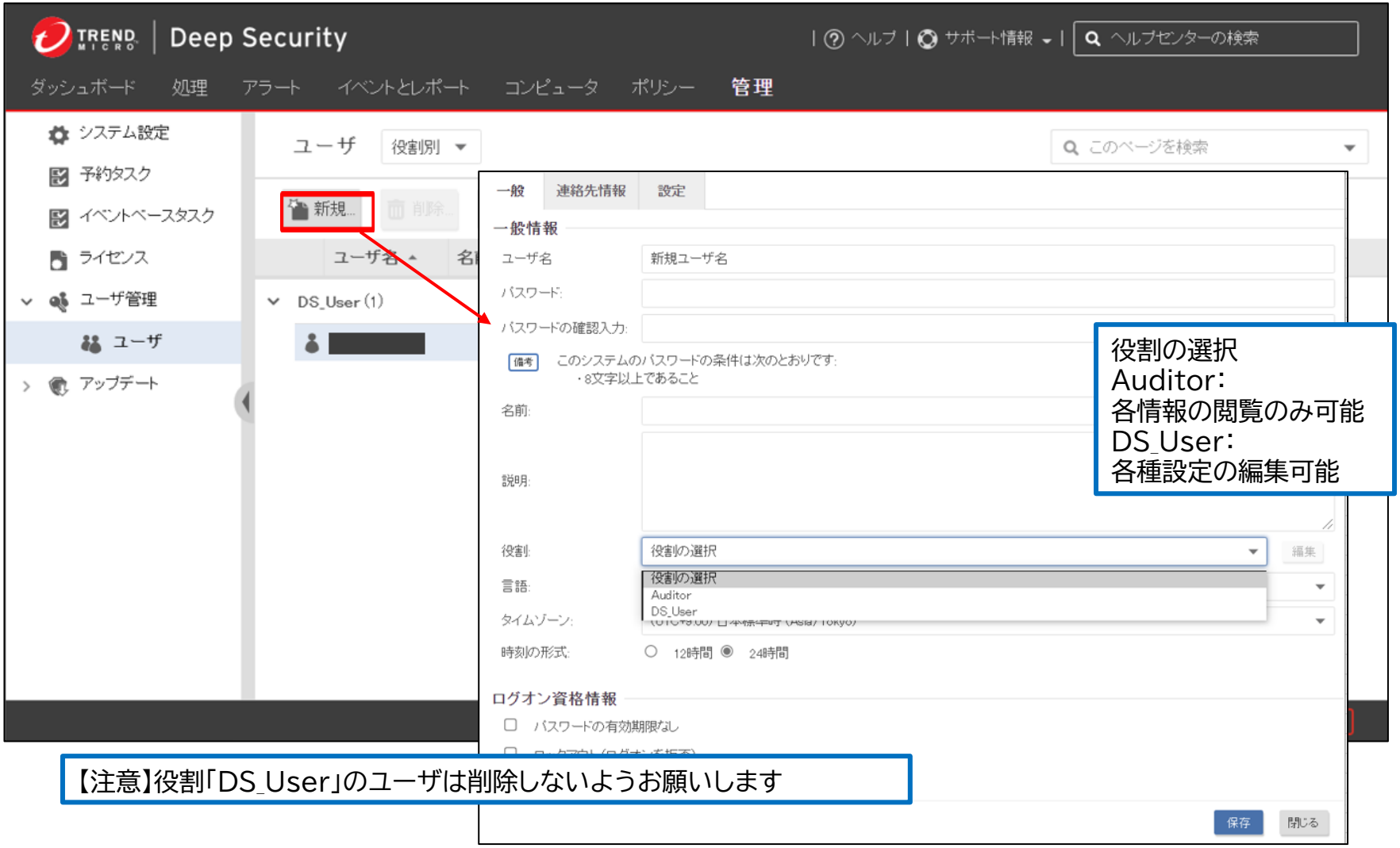
7.管理

- ユーザの管理
  - ユーザの追加･削除やパスワードの設定を行えます。



7.管理

◆ ユーザの新規作成



役割の選択
Auditor：
各情報の閲覧のみ可能
DS_User：
各種設定の編集可能

【注意】役割「DS_User」のユーザは削除しないようお願いします

7.管理

- アップデート
- セキュリティパッチや、ソフトウェアのアップデートの実施・確認を行えます。

8.Apendix

- コマンドラインの利用
- コマンドラインのうち、サーバセキュリティサービスに有用なコマンドを紹介いたします。

Windowsの場合:
・管理者権限でコマンドプロンプトを開きます。
・cd C:¥Program Files¥Trend Micro¥Deep Security Agent¥
・dsa_control オプション

Linuxの場合:
・/opt/ds_agent/dsa_control オプション

1.ハートビートの送信
dsa_control –m ： Managerにハートビートを送り、通信を確立します。

※セキュリティアップデート等、管理コンソール上で行った操作はAgentからハートビートが送信された時に実行されます。(初期設定10分毎)管理コンソール上で行った操作をすぐに実行したい場合は、Agentを導入したサーバで上記のコマンドを実行して下さい。

2.Agentの無効化
dsa_control –r ： Agentを無効化します。

その他のコマンドや詳細につきましては、
https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/command-line-interface.html
をご参照下さい。

8.Apendix

◆ 利用するカーネルに対応したKSPがインポートされているかを確認する方法

1. トレンドマイクロ社が公開しているKSPのReadmeを確認し、
   ご利用しているカーネルに対応したKSPが公開されているか確認ください。

Deep Security のビルド一覧および日本語版Readme
https://success.trendmicro.com/ja-jp/solution/ka-0003376

利用されるDSのバージョンが20.0の場合は「20.0」のリンクをクリック

8.Apendix

2. 利用するカーネルバージョンで検索してください。
   例として「Red Hat Enterprise Linux 7: 3.10.0-1160.71.1.el7.x86_64」の場合
   カーネルバージョン「3.10.0-1160.71.1.el7.x86_64」で検索します。

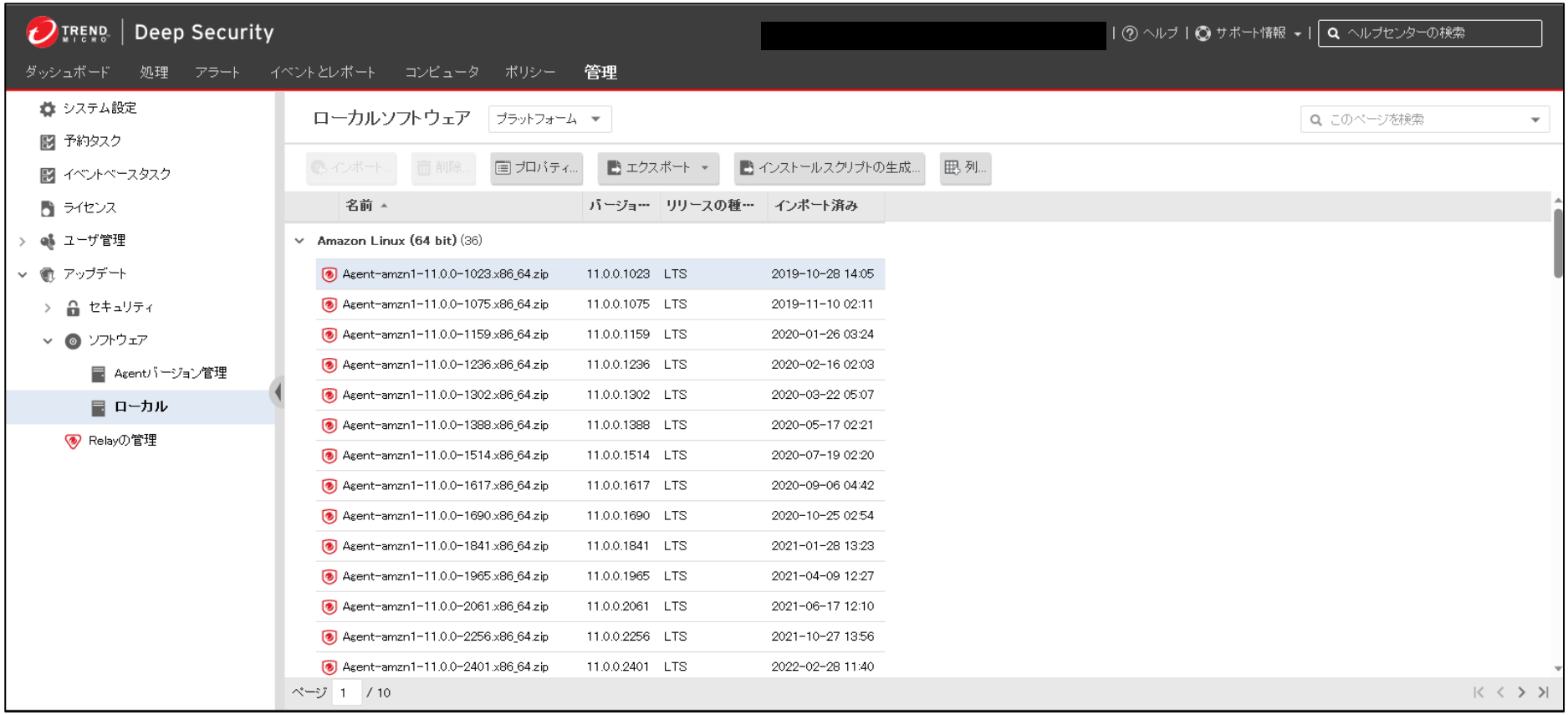
   以下の図では、赤枠で囲った箇所が対応するKSPのバージョンになります。

```
  20.0.0-4984  Jun. 28, 2022
     - KernelSupport-RedHat_EL7-20.0.0-4984.x86_64.zip to support
       Red Hat Enterprise Linux 7: 3.10.0-1160.71.1.el7.x86_64.

  20.0.0-4983  Jun. 28, 2022
     - KernelSupport-RedHat_EL8-20.0.0-4983.x86_64.zip to support
       Red Hat Enterprise Linux 8: 4.18.0-193.87.1.el8_2.x86_64.
```

8.Apendix

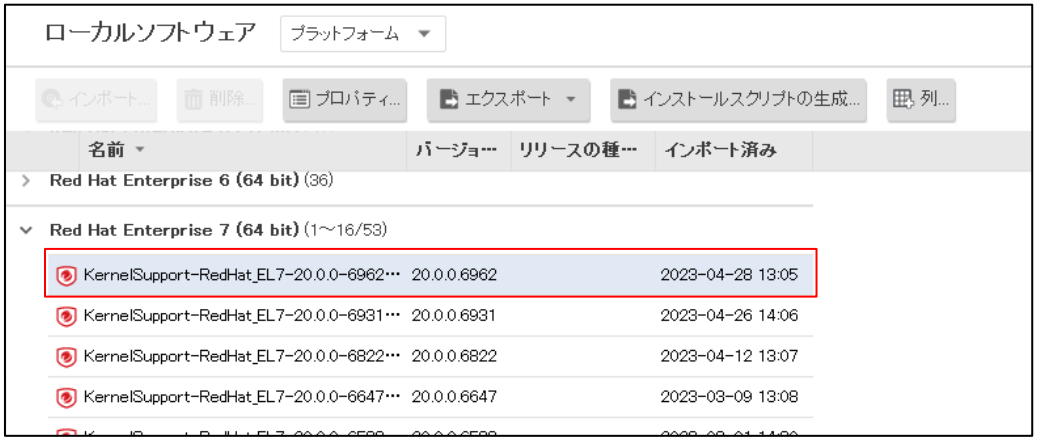
3. サーバセキュリティサービスのDSM管理コンソールにログインし、
   以下の画面を表示します。
   [管理] - [アップデート] - [ソフトウェア] - [ローカル]



8.Apendix

4. 一覧からご利用のOSをクリックして、インポートされている最新KSPをご確認ください。

OSが「Red Hat Enterprise Linux 7」でDSAのバージョンが20.0の場合
「KernelSupport-RedHat_EL7-20.0.0-<ビルド番号>.x86_64.zip」の
<ビルド番号>が一番大きいものを確認します。



手順2で確認したバージョンと一致しているため、利用するカーネルに対応したKSPがインポートされていると判断できます。

新しいKSPには古いKSPのサポートも含まれるため手順2で確認したバージョンより大きい場合も、利用するカーネルに対応したKSPがインポートされていると判断できます。

9.注意事項

- 不正プログラム対策機能をご利用のお客様

不正プログラム対策機能により不審なファイルが隔離された場合、
通信方向が[Agent/Applianceから開始]となっている為、
管理コンソール上では削除できません。
本項では隔離ファイルの処理方法を紹介します。

■ ファイルが隔離処理された場合の対応方法

1. サーバのローカルで隔離ファイルを削除
2. Managerから隔離イベントを削除

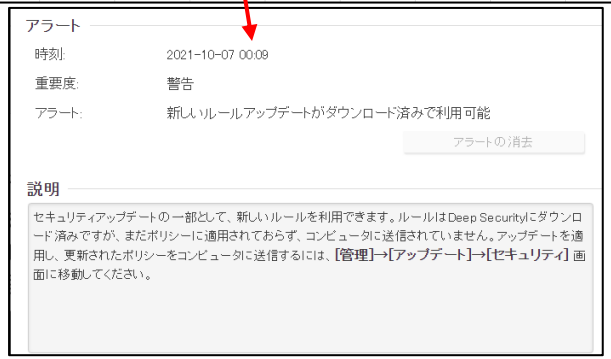
※ 隔離されたファイルは暗号化されてファイル名が変更されるため、
サーバ上で隔離ファイルの生成日時と管理コンソール上の検出ファイルの時刻を
比較してそれぞれ削除が必要となります。

・隔離ファイルや隔離の動作に関するよくあるお問い合わせ
https://success.trendmicro.com/ja-jp/solution/ka-0005972
・通信方向が[Agent/Applianceから開始]の場合の制限事項について
https://success.trendmicro.com/ja-jp/solution/ka-0005792

9.注意事項

- 「新しいルールアップデートがダウンロード済みで利用可能」アラート発生時の対応について

Managerのリソースに対して一時的な負荷が発生し、新しいルールのポリシー反映までに時間を要したためアラートが発令されたと考えられます。
ポリシー反映完了後、アラートは解除されますので対処は不要です。
※アラートメールでは「新しいアラートの発令:新しいルールアップデートが未定用です」の件名でメールが送付されます。



9.注意事項

- Trend Micro Vision One（XDR）について
  バージョン20.0から[管理]＞[システム設定]に[Trend Micro Vision One]タブが
  追加されていますが、本サービスでは提供していませんので触らないようにしてください。

10.問い合わせ先

- 購入済みのお客様
  NEC PPサポートサービスをご利用ください。

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC